Политика выявления, оценки и снижения рисков по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения в системе АКБ «ASIA ALLIANCE BANK»

Policy for identifying, assessing and reducing risks to combat money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction in the system of "ASIA ALLIANCE BANK" JSCB

Tashkent 2023
Ташкент 2023

INDEX

СОДЕРЖАНИЕ

1. General

1.1. The policy for identifying, assessing and reducing risks to combat money laundering, financing of terrorism and proliferation of weapons of mass destruction in the system of "ASIA ALLIANCE BANK" JSCB (hereinafter referred to as the "Policy") is developed in accordance with the Civil Code of the Republic of Uzbekistan, the laws " Concerning the Central Bank of the Republic of Uzbekistan", "Concernin Banks and Banking Activities", "Concerning combating money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction", "Internal Control Regulations for combating money laundering, financing of terrorism and financing proliferation of weapons of mass destruction in commercial banks" (Reg. No. 2886 dated May 23, 2017) and FATF Group recommendations.

1.2. This Policy shall define the procedure for identifying, assessing and reducing risks for all transactions, delivery of banking products to customers, customer's and, representative accounts, new technologies, etc., in order to combat money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction in the system "ASIA ALLIANCE BANK" JSCB (hereinafter referred to as the "Bank").

1.3. The main aim of this Policy is to reduce, prevent and implement modern standards for effective risk management in the field of combating money laundering, financing of terrorism and proliferation of weapons of mass destruction in the provision of banking services.

2. Basic concepts

2.1. This Policy shall use the following basic concepts:

The risk management system is a set of measures taken by the Bank to assess and mitigate risks in the field of combating money laundering, terrorist financing and financing the proliferation of weapons of

1. Общие положения

1.1. Политика выявления, оценки и снижения рисков по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и распространению оружия массового уничтожения в системе АКБ «ASIA ALLIANCE BANK» (далее – «Политика») разработана в соответствии с Гражданским кодексом Республики Узбекистан, законами «О Центральном банке Республики Узбекистан», «О банках и банковской деятельности», «О противодействии легализации преступных доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения», «Правилами внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения в коммерческих банках» (Рег. № 2886 от 23.05.2017) и рекомендациями Группы ФАТФ.

1.2. Настоящая Политика определяет порядок выявления, оценки и снижения рисков по всем операциям, доставке банковских продуктов клиентам, клиентским, представительским счетам, новым технологиям и т.п., в целях противодействия легализации преступных доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения в системе АКБ «ASIA ALLIANCE BANK» (далее – «Банк»).

1.3. Основной целью настоящей Политики является снижение, предотвращение и внедрение современных стандартов эффективного управления рисками в сфере борьбы с отмыванием денег, финансированием терроризма и распространением оружия массового уничтожения при оказании банковских услуг.

2. Основные понятия

2.1. В настоящей Политике используются следующие ключевые понятия:

Система управления рисками - представляет собой комплекс мер, предпринимаемых Банком для оценки и снижения рисков в сфере борьбы с отмыванием денег, финансированием

mass destruction, which will be implemented in the following order:

- Identification of risks and vulnerabilities;
- Risk assessment;
- Management of risks;
- Risk monitoring;
- Inform the Bank's management about the risks.

Identification of risks is identification of sources and causes of risks, taking into account the nature of the risks;

Risk assessment is identification of occurrence of risk factors in transactions and customers for money laundering and terrorist financing;

Risk management means development and implementation of measures to prevent losses associated with risk, including its minimization using the latest technological advances;

Risk monitoring means study, analysis and review of new risks that may arise in order to reduce the risk of money laundering and terrorist financing;

Informing the Bank's management about risks means reducing the likelihood of risks, analyzing and providing information to the Bank's management about new risks that may arise;

customer identification is determination by a commercial bank of data about customers based on documents provided by them, additionally confirmed information available in open sources and databases for the purpose of customer due diligence;

offshore zone - states and territories that provide a preferential tax regime and (or) do not provide for the disclosure and presentation of information when conducting financial transactions;

терроризма и финансированием распространения оружия массового уничтожения, которые будут реализовываться в следующем порядке:

- Выявление рисков и уязвимостей;
- Оценка рисков;
- Управление рисками;
- Мониторинг рисков;
- Информировать руководство Банка о рисках.

Выявление рисков – выявление источников и причин возникновения рисков с учетом характера рисков;

Оценка рисков – выявление случаев возникновения факторов риска в операциях и клиентах по отмыванию денег и финансированию терроризма;

Управление рисками – это разработка и реализация мероприятий по предотвращению потерь, связанных с риском, в том числе их минимизация с использованием новейших технических достижений;

Мониторинг рисков – изучение, анализ и изучение новых рисков, которые могут возникнуть, с целью снижения риска отмывания денег и финансирования терроризма;

Информирование руководства Банка о рисках – снижение вероятности возникновения рисков, анализа и предоставление информации руководству Банка о новых рисках, которые могут возникнуть;

идентификация клиента – определение коммерческим банком данных о клиентах на основе предоставленных ими документов, дополнительно подтвержденных сведений, доступных в открытых источниках и базах данных в целях надлежащей проверки клиента;

оффшорная зона – государства и территории, предоставляющие льготный налоговый режим и (или) не предусматривающие раскрытие и представление информации при проведении финансовых операций;

Specially Authorized State Body is a special Department for Organized Crime, Economic Crime and Corruption at the General Prosecutor's Office of the Republic of Uzbekistan (hereinafter referred to as the Department);

Специально уполномоченный государственный орган — Департамент по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан (далее – Департамент);

List means a list of persons participating or suspected of participating in terrorist activities or proliferation of weapons of mass destruction, generated by a specially authorized state body based on information provided by state bodies engaged in combating terrorism, proliferation of weapons of mass destruction, and other competent authorities of the Republic of Uzbekistan, and also information received through official channels from the competent authorities of foreign states and international organizations.

Перечень — перечень лиц, участвующих или подозреваемых в участии в террористической деятельности или распространении оружия массового уничтожения, формируемый специально уполномоченным государственным органом на основании сведений, представляемых государственными органами, осуществляющими борьбу с терроризмом, распространением оружия массового уничтожения, и другими компетентными органами Республики Узбекистан, а также сведений, полученных по официальным каналам от компетентных органов иностранных государств и международных организаций.

states not participating in international cooperation in the field of combating money laundering and financing of terrorism means states and territories identified in the official statements of the Financial Action Task Force on Money Laundering, which pose a threat to the international financial system and whose system for combating money laundering and financing of terrorism has strategic shortcomings;

государства, не участвующие в международном сотрудничестве в сфере противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма — государства и территории, определенные в официальных заявлениях Группы по разработке финансовых мер борьбы с отмыванием денег, которые представляют угрозу международной финансовой системе и у которых система противодействия легализации доходов, полученных от преступной деятельности и финансированию терроризма, имеет стратегические недостатки;

remote services are banking services provided for conducting transactions using programs that make it possible to carry out transactions without the customer appearing at a commercial bank.

дистанционные услуги — банковские услуги, предоставляемые по проведению операций с использованием программ, дающих возможность осуществления операций без явки клиента в коммерческий банк.

3. Identification of risks and vulnerabilities

3. Выявление рисков и уязвимостей

3.1. Risk assessment for combating money laundering and terrorist financing is important in setting priorities in this area in the process of providing banking services and products, and implies paying special attention to high-risk transactions and customers.

3.1. Оценка рисков по противодействию легализации преступных доходов и финансированию терроризма имеет важное значение при определении приоритетов в данной сфере в процессе предоставления банковских услуг и продуктов, и подразумевает уделение особого внимания высоко рисковым операциям и клиентам.

3.2. To identify the Bank's exposure to the risk

3.2. Для выявления подверженности Банка риску

of money laundering and terrorist financing, the Bank shall consider the following factors:

– the nature and scope of operations of the Bank's activities;
– target markets;
– the volume and size of the Bank's operations, taking into account the normal activities and customers profile;
– the number of customers classified as high risk;
– jurisdictions with which the Bank works directly or through the activities of customers;
– service delivery channels, taking into account the degree of direct work with the customer (remote service, customer due diligence by third parties, the use of technology);
– results of internal and external audit;
– information coming from the Central Bank and the Department.

отмывания денег и финансирования терроризма, Банк учитывает следующие факторы:

– характер и объем операций деятельности Банка;
– целевые рынки;
– объем и размер операций Банка, с учетом обычной деятельности и профиля клиентов;
– количество клиентов, отнесенных к категории высокого риска;
– юрисдикции, с которыми работает Банк напрямую или через деятельность клиентов;
– каналы предоставления услуг, с учетом степени непосредственной работы с клиентом (дистанционное обслуживание, проведение надлежащий проверок клиентов третьими лицами, использование технологий);
– результаты внутреннего и внешнего аудита;
– информации, поступающей от Центрального банка и Департамента.

3.3. Organizational-systemic risk assessment shall be carried out in accordance with established measures, where the availability of resources and information is important.

The risk assessment in the provision of banking services and products shall depend on the extent to which they are exposed to risk and protected. Including:

– risk associated with the scale and nature of the risk in the field of combating money laundering and financing of terrorism;
– technological or operational risk (Vulnerability) caused by insufficient attention to measures to prevent the risks of newly provided or improved banking services.

3.3. Организационно-системная оценка рисков осуществляется в соответствии с установленными мерами, при которых важное значение имеет доступность ресурсов и информации.

Оценка рисков при предоставлении банковских услуг и продуктов зависит от того, в какой степени они подвержены риску и защищены. В том числе:

– риск, связанный с масштабом и характером риска в сфере противодействия легализации доходов, полученных преступным путем и финансированию терроризма;
– технологический или операционный риск (Уязвимость), вызванный недостаточным вниманием к мерам по предотвращению рисков вновь предоставляемых или улучшаемых банковских услуг.

3.4. Vulnerabilities and risks in the provision of banking services and products can be caused by the following factors:
The use of multiple methods of disposal, management, delivery, transfer and receipt of funds by persons using banking services, including persons included in the List, shall complicate the process of

3.4. Уязвимости и риски при предоставлении банковских услуг и продуктов могут быть вызваны следующими факторами:
Использование множественных методов распоряжения, управления, доставки, перевода и получения денежных средств лицами, пользующимися банковскими услугами, в том числе лицами, включенными в

assessing the main risks of money laundering and terrorist financing. They may use legal and illegal sources of income to achieve their malicious goals. In particular:

Перечень, усложняет процесс оценки основных рисков отмывания денег и финансирования терроризма. Они могут использовать легальные и нелегальные источники дохода для достижения своих злонамеренных целей. В частности,

By embezzling funds from legitimate sources: financing and supporting groups engaged in money laundering or terrorist activities from legitimate sources, using funds from various charitable and commercial organizations - usually in such cases, groups use the method of self-financing by attracting an employee who works at the expense of such funds and social payments. As a result, operations that appear legitimate are unsuspicious practices.

Путем присвоения средств из законных источников: финансирование и поддержка групп, занимающихся отмыванием денег или террористической деятельностью из законных источников, использование средств различных благотворительных и коммерческих организаций – обычно в таких случаях группы используют метод самофинансирования путем привлечения наемного лица, которое работает за счет таких фондов и социальных выплат. В результате операции, которые кажутся законными, являются не вызывающими подозрений методами.

Using proceeds of crime: Money laundering or terrorist groups often turn to illegal sources of funding, including arms and drug trafficking, human trafficking, hostage taking, extortion, fraud, intrusion and smuggling.

Путем использования доходов от преступной деятельности: группы, занимающиеся отмыванием денег или террористической деятельностью, часто прибегают к противоправным источникам финансирования, включая незаконный оборот оружия и наркотиков, торговлю людьми, захват заложников, вымогательство, мошенничество, вторжение и контрабанду.

Through the use of state support: assistance to refugees from hostilities in various countries, sponsor countries in need of economic and social support, is one of the main sources of funding for groups involved in money laundering or terrorist activities. In such cases, they are used to transfer and remit funds to countries with a large number of refugees, weak judicial oversight and insufficient control over the movement of funds.

За счет использования государственной поддержки: помощь беженцам от военных действий в различных странах, странах-спонсорах, нуждающихся в экономической и социальной поддержке, являются одним из основных источников финансирования групп, занимающихся отмыванием денег или террористической деятельностью. В таких случаях они используются для перечисления и перевода денежных средств странами с большим количеством беженцев, слабым судебным надзором и недостаточным контролем за движением средств.

3.5. Regular assessment of risks (vulnerabilities) and vulnerabilities arising from these situations, and taking measures to eliminate them is of particular importance in risk management. Therefore, all operations, including currency exchange operations, methods of delivering banking products to customers, regular monitoring of customers,

3.5. Регулярная оценка рисков (уязвимостей) и уязвимостей, возникающих этих ситуаций, и принятие мер по их устранению имеет особое значение в управлении рисками. Поэтому все операции, включая валютно-обменные операции, способы доставки банковских продуктов клиентам, регулярный мониторинг клиентов, корреспондентских счетов, должны быть проанализированы для оценки

correspondent accounts, should be analyzed to assess existing risks and vulnerabilities, and measures should be taken to eliminate, prevent and reduce (minimize) them.

In this regard, the study of foreign exchange transactions, in particular international and non-cash transfers, export-import transactions, their sources, channels and implementation processes, based on the degree of risk, is a priority task in identifying risks.

4. Risk assessment

4.1. Responsible personnel of the Compliance Control Department will take appropriate measures to identify, evaluate, monitor, manage, document and reduce the level of risk.

Depending on the type and level of risks, its general level, the required level of its reduction should be determined and an appropriate program of measures should be implemented.

The level of risk is based on the operations conducted by the customer, the criteria defined in the "Internal Control Regulations for Combating Money Laundering, Financing of Terrorism and Financing the Proliferation of Weapons of Mass Destruction in the ASIA ALLIANCE BANK System" (hereinafter referred to as the Internal Regulations) and the results of customer due diligence, based on information, provided by the customer on a risk-sensitive basis (customers, countries and geographic areas, and product and service channels) shall be determined and evaluated by the responsible officer of the Compliance Control Department.

4.2. Responsible personnel should give increased attention to customers that meet the following criteria by assigning them a high-risk category:

a) persons on the List or entities owned or controlled by a person on the List, or persons directly or indirectly owning or controlling an entity on the List;

существующих рисков и уязвимостей, а также должны быть приняты меры по их устранению, предотвращению и уменьшению (минимизации).

В связи с этим изучение валютных операций, в частности международных и безналичных переводов, экспортно-импортных операций, их источников, каналов и процессов осуществления, исходя из степени риска, является приоритетным задачам при выявлении рисков.

4. Оценка рисков

4.1. Ответственные персоналы Управления комплаенс-контроля будут принимать соответствующие меры для выявления, оценки, мониторинга, управления, документирования и снижения уровня риска.

В зависимости от вида и уровня рисков следует определить их общий уровень, требуемый уровень его снижения и реализовать соответствующую программу мероприятий.

Уровень риска основан на проводимых клиентом операциях, критериях, определенных в «Правилах внутреннего контроля по противодействию легализации преступных доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения в системе ASIA ALLIANCE BANK» (далее – Внутренние правила) и результаты надлежащей проверки клиента, на основании информации, предоставленной клиентом, с учетом факторов риска связанных с клиентом и операцией (клиенты, страны и географические районы, а также каналы продуктов и услуг) определяется и оценивается ответственным сотрудником Управления комплаенс-контроля.

4.2. Ответственный персонал должен уделять повышенное внимание клиентам, отвечающим следующим критериям, присваивая им категорию высокого риска:

а) лица, включенные в Перечень либо организации, находящиеся в собственности или под контролем лица, включенного в Перечень, либо лица, прямо или косвенно являющиеся собственниками

b) persons permanently residing, staying or registered in a state that does not participate in international cooperation in the field of combating money laundering and the financing of terrorism;

c) Representative offices of foreign companies and non-residents - individuals of the Republic of Uzbekistan;
d) persons permanently residing, located or registered in an offshore zone;
e) residents and non-residents with accounts in offshore zones;
f) organizations and individual entrepreneurs, which actual location does not correspond to the information specified in the constituent or registration documents;

g) organizations, the beneficial owner of which is the person specified in paragraphs "a" and "b" of this clause;

h) customers who carry out suspicious or doubtful transactions on a systematic basis (for example, within 3 consecutive months);
i) customers using software systems that exclude the possibility of customer due diligence;

j) public officials, members of their families and persons close to public officials;
k) Persons of whom the Bank is aware that they are included in the current lists of the UN (in accordance with resolutions of the Security Council) and the Office of Foreign Assets Control of the US Department of the Treasury (OFAC SDN list).
l) Organizations and individual entrepreneurs who have established new business relations with the Bank for no more than 3 months;

4.3. Executive officers should classify transactions that meet the following criteria as high-risk and give them increased attention:

или контролирующие организацию, включенную в Перечень;
b) лица, постоянно проживающие, находящиеся или зарегистрированные в государстве, не участвующем в международном сотрудничестве в в области противодействия легализации доходов, полученных от преступной деятельности, и финансированию терроризма;
c) Представительства иностранных компаний и нерезиденты – физические лица Республики Узбекистан;
d) лица, постоянно проживающие, находящиеся или зарегистрированные в оффшорной зоне;
e) резиденты и нерезиденты, имеющие счета в оффшорных зонах;
f) организации и индивидуальные предприниматели, фактическое местонахождение которых не соответствует сведениям, указанным в учредительных или регистрационных документах;
g) рганизации, бенефициарным собственником которых является лицо, указанное в подпунктах «а» и «б» настоящего пункта;
h) клиенты, осуществляющие подозрительные или сомнительные операции на систематической основе (например, в течение 3 месяцев подряд);
i) клиенты, использующие программные комплексы, исключающие возможность осуществления надлежащей проверки клиента;
j) публичные должностные лица, члены их семей и лица, близкие к публичным должностным лицам;
k) Лица, о которых Банку известно, что они включены в действующие списки ООН (в соответствии с резолюциями Совета Безопасности) и Управления по контролю за иностранными активами Министерства финансов США (список OFAC SDN).

l) Организации и индивидуальные предприниматели, установившие новые деловые отношения с Банком не более чем на 3 месяца;

4.3. Должностным лицам следует классифицировать операции, отвечающие следующим критериям, как высокорисковые и уделять им повышенное внимание:

a) transactions, the participants of which are the persons specified in paragraphs "a", "b", "h" and "l" Clause 4.2 of this Policy;
b) transactions carried out through accounts opened in an offshore zone;
c) transactions with precious metals, precious stones, as well as jewelry containing precious metals, precious stones, with the exception of such transactions carried out by commercial banks themselves;
d) Operations involving the transfer of funds, in which information about the sender (last name, first name, patronymic of individuals, name of legal entities, location of the sender (postal address) and account number) is not specified in full;

a) сделки, участниками которых являются лица, указанные в подпунктах «а», «б», «з» и «л» пункта 4.2 настоящей Политики;
b) операции, осуществляемые через счета, открытые в оффшорной зоне;
c) операции с драгоценными металлами, драгоценными камнями, а также ювелирными изделиями, содержащими драгоценные металлы, драгоценные камни, за исключением таких операций, осуществляемых самими коммерческими банками;
d) Операции, с переводом денежных средств, при которых сведения об отправителе (фамилия, имя, отчество физических лиц, наименование юридических лиц, место нахождения отправителя (почтовый адрес) и номер счета) не указана в полном объеме;

4.4. When a customer, or a transaction carried out by a customer, is classified as high risk, responsible personnel must apply enhanced due diligence measures to that customer.

4.4. При отнесении клиента или операции, осуществляемой клиентом, к категории высокого уровня риска, ответственный персонал должен применять усиленные меры по надлежащей проверке в отношении такого клиента.

4.5. Depending on changes in the nature of the transactions conducted by the customer, internal control officers in the branches, if necessary, should review the level of risk of working with the customer.

4.5. В зависимости от изменений характера проводимых клиентом операций сотрудники внутреннего контроля в филиалах при необходимости должны пересматривать уровень риска работы с клиентом.

4.6. In all branches, an internal control officer shall maintain a record of customers classified as high-risk.

4.6. Во всех филиалах сотрудник внутреннего контроля ведет учет клиентов, отнесенных к категории высокого уровня риска.

4.7. The Bank must take measures to prevent the use of technological advances for the purposes of money laundering or terrorist financing. To this end, the Bank shall take all necessary measures to study and eliminate the risks and vulnerabilities that may arise from:

– introduction of new types of services and provision of banking products;
– introduction of new or improved technologies for new and existing types of services.

4.7. Банк должен принять меры для предотвращения использования технологических достижений в целях легализации доходов, полученных преступным путем или финансирования терроризма. С этой целью Банк должен принять все необходимые меры для изучения и устранения рисков и уязвимостей, которые могут возникнуть в результате:
– внедрения новых видов услуг и предоставления банковских продуктов;
– внедрения новых или усовершенствованных технологий для новых и существующих видов услуг.

4.8. Such a risk assessment should be carried out immediately before the introduction of new services and banking products, by

4.8. Такая оценка рисков должна проводиться непосредственно перед внедрением новых услуг и банковских продуктов, внедрением в

introduction of new or improved technologies into practice. Identification and assessment of risks shall be carried out by a division that directly introduces new types of services and new technologies of the bank together with the Compliance Control Department.

практику новых или усовершенствованных технологий. Выявление и оценка рисков осуществляется подразделением, которое непосредственно внедряет новые виды услуг и новые технологии банка совместно с Управлением комплаенс-контроля.

5. Risk management

5.1. Risk management is a set of measures taken by the Bank to assess and mitigate money laundering or terrorist financing risks.

The Bank's risk management is based on a risk-based approach, which allows it to take measures to combat money laundering and terrorist financing.

5.2. In order to manage risks, the Compliance Control Department of the Bank must take the following measures:

- examine banking services and products that may pose a high risk in order to identify and assess the level of risk;
- in order to reduce (minimize) risks, make proposals to the structural divisions of the Bank to prevent risks and eliminate identified vulnerabilities.

5.3. When managing risks, special and sufficient attention should be paid to customers belonging to the high-risk category, as well as customers with the following risk factors:

- use of banking services directly without visiting the Bank;
- use of remote banking services;
- use of legal entities to manage personal funds;
- customers - legal entities having nominee shareholders or bearer shares;
- customers with an unusual or unnecessarily complex company ownership structure, given the nature of the business;
- customers who use cash intensively.

5.4. The Bank shall take the following risk

5. Управление рисками

5.1. Управление рисками – это комплекс мер, предпринимаемых Банком для оценки и снижения рисков отмывания денег или финансирования терроризма.

Управление рисками Банка основано на риск-ориентированном подходе, что позволяет принимать меры по борьбе с отмыванием денег и финансированием терроризма.

5.2. 5.2. В целях управления рисками Управление комплаенс-контроля Банка должно принять следующие меры:

- изучить банковские услуги и продукты, которые могут представлять высокий риск, с целью выявления и оценки уровня риска;
- в целях снижения (минимизации) рисков вносить предложения в структурные подразделения Банка по предотвращению рисков и устранению выявленных уязвимостей.

5.3. При управлении рисками особое и достаточное внимание должно уделяться клиентам, относящимся к категории высокого уровня риска, а также клиентам, имеющим следующие факторы риска:

- использование банковских услуг непосредственного без посещения Банка;
- использование дистанционных банковских услуг;
- использование юридических лиц для управления личными средствами;
- клиентам юридическим лицам, имеющим номинальных акционеров или акции на предъявителя;
- клиенты с необычной или излишне сложной структорой собственности компании, учитывая характер деятельности;
- клиенты, интенсивно использующие наличную форму расчетов.

5.4. Банком принимаются следующие меры по

management measures when providing remote banking services, including:

- measures taken in case of detection of suspicious transactions performed by the customer using these services in contracts executed with customers for the provision of remote services (suspension of the provision of these services until the customer provides a written explanation of the legality of the transaction; refusal to provide these services);

- if there are doubts about the conduct of suspicious transactions using remote services, a special committee with the participation of a responsible employee of the branch shall establish the fact that transactions have been carried out by the person specified in the Remote Service Agreement, examine the customer at the location (postal address) or address specified in the Remote Services Agreement;

- suspend the provision of remote services, which were used to carry out suspicious transactions, for the period specified in the contract for the provision of this service;

- if there are reasonable suspicions that remote services are used for money laundering and terrorist financing purposes, terminate contracts for the provision of such services in the prescribed manner.

5.5. When examining a customer using remote services, at his location (postal address) or the address specified in the Remote Services Agreement, the Bank must pay special attention to the customer's compliance with the requirements of the Regulation on cashless payments in the Republic of Uzbekistan (No. 3229 dated 13.04.2020), including the execution of settlement documents, its certification by the signature of authorized persons (Manager, Chief Accountant), the implementation of transfers on these documents only after confirmation by an electronic digital signature by a person directly entitled to an electronic signature,

управлению риском при оказании дистанционного банковского обслуживания, в том числе:

- меры, принимаемые в случае выявления подозрительных операций, совершенных клиентом с использованием данных услуг в договорах, заключенных с клиентами на оказание дистанционных услуг (приостановление оказания данных услуг до предоставления клиентом письменного объяснения законности совершения операции; отказ в предоставлении данных услуг);

- при наличии сомнений о проведении подозрительных операций с использованием дистанционных услуг специальная комиссия с участием ответственного работника филиала устанавливает факт проведения операций лицом, указанным в договоре дистанционного обслуживания, изучает клиента по месту нахождения (почтового адреса) или адресу, указанного в договоре об оказании дистанционных услуг;

- приостанавливать предоставление дистанционных услуг, с использованием которых осуществлялись подозрительные операции, на срок, указанный в договоре об оказании данной услуги;

- при наличии обоснованных подозрений в использовании дистанционных услуг в целях отмывания денег и финансирования терроризма расторгнуть в установленном порядке договоры на оказание таких услуг.

5.5. При изучении клиента, пользующегося дистанционными услугами, по месту его нахождения (почтовому адресу) или адресу, указанному в договоре об оказании дистанционных услуг, Банк должен уделять особое внимание соблюдению клиентом требований Положения о безналичных расчетах в Республике Узбекистан (№ 3229 от 13.04.2020 г.), в том числе оформлению расчетных документов, их заверению подписью уполномоченных лиц (руководителя, главного бухгалтера), осуществлению переводов по этим документам только после подтверждения электронно-цифровой подписью лицом, непосредственно имеющим право на

storage of these documents.

5.6. Particular attention should be paid to the fact that all information is requested and identified to identify the customers themselves and beneficiaries whose bank accounts are opened remotely. In order to mitigate the risks, the branch of the Bank serving the customer, if necessary, must take measures to verify the customer.

5.7. In order to prevent possible risks, the Bank shall not enter into correspondent relations:

- with “nominal” banks (banks registered in a jurisdiction in which they do not have a physical presence and are not associated with a regulated financial group);
- if, on the basis of information collected in accordance with the requirements of the Internal Rules, it cannot be sure that the correspondent is not a “nominal bank”.

The Bank does not provide permission to use its correspondent accounts directly or indirectly to third parties (“transit” accounts – payable through).

In order to prevent possible risks, the Bank does not open, maintain and does not continue to service anonymous bank accounts. The Bank does not issue or service bearer financial instruments. The Bank does not make payments to such accounts.

6. Risk monitoring

6.1. The Compliance Control Department of the Bank shall take appropriate measures to monitor and mitigate risks.

Risk monitoring in all branches shall be carried out by responsible employees of the Compliance Control Department in the branches and direct customer service personnel.
Responsible employees of the Compliance Control Department shall be responsible for establishing enhanced control over customers and operations with a high level of risk.

электронную подпись, хранению данных документов.

5.6. Особое внимание следует обратить на то, что вся информация запрашивается и идентифицируется для идентификации самих клиентов и бенефициаро, чьи банковские счета открыты удаленно. В целях снижения рисков отделение Банка, обслуживающее клиента, при необходимости должно принять меры по проверке клиента.

5.7. В целях предотвращения возможных рисков Банк не вступает в корреспондентские отношения:

- с «номинальными» банками (банки, зарегистрированные в юрисдикции, в которой они не имеют физического присутствия и не связаны с регулируемой финансовой группой);
- если на основании информации, собранной в соответствии с требованиями Внутренних правил, не может убедиться, что корреспондент не является «номинальным банком».

Банк не предоставляет разрешений по использованию своих корреспондентских счетов прямо или косвенно третьим лицам («транзитные» счета – payable through).

В целях предотвращения возможных рисков Банк не открывает, не ведет и не продолжает обслуживать анонимные банковские счета. Банк не выпускает и не обслуживает финансовые инструменты на предъявителя. Банк не проводит платежи на такие счета.

6. Мониторинг рисков

6.1. Управление комплаенс-контроля Банка должен принимать соответствующие меры для мониторинга и снижения рисков.

Мониторинг рисков во всех филиалах осуществляется ответственными работниками Управления комплаенс-контроля в филиалах и непосредственным персоналом по работе с клиентами.
Ответственные работники Управления комплаенс-контроля несут ответственность за установление усиленного контроля за клиентами и операциями, с высоким уровнем риска.

Different monitoring methods can be used depending on the level and frequency of risks, the scope of work.

The Compliance Control Department of the Bank shall control the monitoring of risks through responsible employees of the Bank's branches in order to combat money laundering and financing of terrorism.

В зависимости от уровня и периодичности рисков, объема работ могут использоваться разные методы мониторинга.

Управление комплаенс-контроля Банка контролирует осуществление мониторинга рисков ответственными сотрудниками филиалов Банка в целях противодействия легализации доходов, полученных преступным путем, и финансированию терроризма.

6.2. In order to ensure the bank's effectiveness in combating money laundering and terrorist financing, the Bank's Compliance Control Department may generate reports that allow the bank's program to automatically identify suspicious and suspicious transactions.

6.2. В целях обеспечения эффективности банка в борьбе с отмыванием денег и финансированием терроризма Управление комплаенс-контроля Банка может формировать отчеты, позволяющие программе банка автоматически выявлять подозрительные и подозрительные операции.

6.3. In addition to the introduction of banking services provided to customers, the Bank shall take measures to continuously improve its software to ensure the Bank's effectiveness in combating money laundering and terrorist financing, as well as to effectively monitor and identify risks.

6.3. Помимо внедрения банковских услуг, предоставляемых клиентам, Банк принимает меры по постоянному совершенствованию своего программного обеспечения для обеспечения эффективности Банка в сфере противодействия легализации доходов, полученных преступным путем, и финансированию терроризма, а также для эффективного мониторинга и выявления рисков.

6.4. The requirements of the Internal Control Rules must be included in the job descriptions of employees responsible for direct customer service in all divisions and branches of the Bank. This requirement requires all responsible employees to monitor customer transactions and accounts when serving customers, and to pay increased attention to customers and high-risk transactions.

Executive officers who do not comply with these requirements shall be considered as violated the internal labor regulations and shall be held liable.

6.4. Требования Правил внутреннего контроля должны быть включены в должностные инструкции работников, ответственных за непосредственное обслуживание клиентов во всех подразделениях и филиалах Банка. Это требование требует, чтобы все ответственные сотрудники контролировали транзакции и счета клиентов при обслуживании клиентов, а также уделяли повышенное внимание клиентам и транзакциям с высоким риском.

Должностные лица, не соблюдающие данные требования, считаются нарушившими правила внутреннего трудового распорядка и будут привлечены к ответственности.

6.5. The division of the Bank that provides the relevant services or products shall be responsible for eliminating shortcomings and vulnerabilities identified during risk monitoring and taking measures to prevent such situations.

6.5. Подразделение Банка, оказывающее соответствующие услуги или предоставляющее продукты, несет ответственность за устранение недостатков и уязвимости, выявленных в ходе мониторинга рисков, и принятие мер по предотвращению таких ситуаций.

7. Providing information to the management of the bank about the risks

7.1. The Compliance Control Department, together with the Bank's subdivisions, shall provide the Bank's Management Board with information on monitoring risks in the area of combating money laundering and terrorist financing.

7.2. In order to identify and eliminate risks (vulnerabilities) associated with the introduction of new or improved technologies when introducing new types of services and products of the Bank, the Compliance Control Department, together with the division that directly introduces new types of services and new technologies, shall inform the Bank's management and make appropriate proposals.

8. Final provisions

8.1. This Policy is mandatory for execution by all structural subdivisions and branches of the Bank.

8.2. Monitoring and control over compliance with the requirements of this Policy in the Bank and its branches shall be carried out by the Compliance Control Department.

8.3. This Policy shall come into force from the date of its approval by the Supervisory Board of the Bank, and from the same date the Policy approved by No. K-21/2 Minutes of the Meeting of the Supervisory Board of the Bank dated November 1, 2021, shall be considered invalid.

8.4. The original of this Policy is made in Uzbek and Russian. At the same time, in case of any discrepancy, the text in Uzbek shall prevail.

7. Предоставление информации руководству банка о рисках

7.1. Управление комплаенс-контроля совместно с подразделениями Банка предоставляет Правлению Банка информацию о мониторинге рисков в сфере противодействия легализации доходов, полученных преступным путем, и финансированию терроризма.

7.2. В целях выявления и устранения рисков (уязвимостей), связанных с внедрением новых или усовершенствованных технологий при внедрении новых видов услуг и продуктов Банка, Управление комплаенс-контроля совместно с подразделением, непосредственно внедряющим новые виды услуг и новых технологий, информирует руководство Банка и вносит соответствующие предложения.

8. Заключительные положения

8.1. Настоящая Политика обязательна для исполнения всеми структурными подразделениями и филиалами Банка.

8.2. Мониторинг и контроль за соблюдением требований настоящей Политики в Банке и его филиалах осуществляет Управление комплаенс-контроля.

8.3. Настоящая Политика вступает в силу с даты ее утверждения Наблюдательным советом Банка, а с этой же даты Политика, утвержденной протоколом заседания Наблюдательного совета Банка № К-21/2 от 01.11.2021 г., считается утратившей силу.

8.4. Оригинал настоящей Политики составлен на узбекском и русском языках. При этом в случае любого разночтения преимущественную силу имеет текст на узбекском языке.